Forum Standaardisatie

Wilhelmina van Pruisenweg 52
2595 AN Den Haag

Postbus 96810
2509 JE Den Haag

www.forumstandaardisatie.nl

notitie

FORUM STANDAARDISATIE

Agendapunt:			
Betreft:	Intake-advies voor DANE en STARTTLS		
Aan:	Forum Standaardisatie		
Van:	Stuurgroep Open Standaarden		
Datum:	16 december 2015	**Versie**	1.0

Bijlagen: -

Advies

Het Forum Standaardisatie wordt geadviseerd om DNS-Based Authentication of Named Entities (DANE) en STARTTLS, standaarden voor de transportbeveiliging van e-mail, in behandeling te nemen voor opname op de lijst met standaarden.

In procedure nemen van deze standaarden is van belang vanwege de risico's die via niet-versleutelde verbindingen kunnen ontstaan, zoals het 'afluisteren' en manipuleren van berichtenverkeer. DANE en STARTTLS zorgen ervoor dat elektronische gegevensuitwisseling (e-mail) tussen mailservers via een beveiligde verbinding wordt verstuurd.

Betrokkenen en Proces

In 2013 is een toetsingsprocedure doorlopen voor DANE. Omdat DANE nog zeer beperkt werd toegepast en de marktondersteuning voor de toepassing van DANE onvoldoende was, heeft de expertgroep geadviseerd om de standaard niet op te nemen op de lijst voor pas toe of leg uit. Onderdeel van het advies was om na een bepaalde periode en op aangeven van de indiener de adoptie van de standaard opnieuw te beoordelen.

DANE is ingediend door NLnet. In het gesprek met de indiener is naar voren gekomen dat DANE in toenemende mate wordt toegepast met STARTTLS om een beveiligde verbinding tussen mailservers op te kunnen zetten. Daarom wordt op aangeven van de indiener zowel voor DANE als STARTTLS een uitgebreide procedure uitgevoerd worden, waarbij voor DANE ook een aanvullend onderzoek wordt gedaan naar de adoptie van de standaard.

Beide standaarden voldoen aan de criteria voor inbehandelname. Mede door de toepasbaarheid van de standaarden en de relatie tot een aantal andere internet- en e-mailbeveiligingsstandaarden is de kansrijkheid van de procedure voldoende.

De aanmelding van DANE en STARTTLS als open standaarden wordt ondersteund door het Nationaal Cyber Security Centrum (NCSC) en SURFnet. Het is tijdens de intake niet duidelijk of één van deze partijen de standaarden ook hebben geïmplementeerd. In Nederland maken Netlabs en Forum Standaardisatie gebruik van beide standaarden. In Duitsland, Noorwegen en Amerika worden beide standaarden op grotere schaal toegepast.

Aandachtspunten tijdens de procedure
Geadviseerd wordt om tijdens de expertbijeenkomst stil te staan bij de adoptie van de standaarden binnen het organisatorisch werkingsgebied, met name voor DANE is dit minder inzichtelijk. Daarnaast zal gekeken moeten worden of de standaarden verplicht of aanbevolen moet worden gesteld. Daarnaast dient tijdens de expertbijeenkomst aandacht te worden besteed aan de implementatiekosten van STARTTLS en DANE. Ook kennen DANE en STARTTLS een relatie met DNSSCEC en TLS en de e-mailstandaarden DKIM, SPF en DMARC. Het is goed om tijdens de procedure deze relaties goed inzichtelijk te maken zodat duidelijk wanneer welke standaard te gebruiken.

Toelichting

1. Aanmelding, intakegesprek en toetsingsprocedure

Op 29 oktober 2015 is door Michiel Leenaars van NLnet de standaard DANE aangemeld voor de lijst met open standaarden. De aanmelder heeft als doel de standaard verplicht (‘pas-toe-of-leg-uit’) te stellen.

Op 17 november 2015 heeft een intakegesprek plaatsgevonden met de aanmelder van DANE. In dit gesprek is de aanmelding besproken. Hierbij is gekeken of alle basisinformatie aanwezig is en of de standaard voldoet aan de criteria voor inbehandelname. Daarnaast is vooruitgeblikt op de procedure. Naar aanleiding van dit gesprek bleek ook STARTTLS een belangrijke toevoeging te zijn.

2. Korte beschrijving standaard

Waar gaan de standaarden over?

STARTTLS

E-mails worden door de mailserver van de verzendende mailprovider verstuurd naar de mailserver van de ontvangende partij. De verbinding tussen deze mailservers kan versleuteld worden door middel van TLS. De standaard STARTTLS upgrade een niet-versleutelde, en daarmee onbeveiligde, verbinding naar een versleutelde TLS-verbinding. Met de versleutelde TLS-verbinding wordt voorkomen dat een passieve aanvaller het berichtenverkeer 'afluistert'. Een passieve aanvaller manipuleert het berichtenverkeer niet, zoals het onderscheppen van e-mails. Om STARTTLS in werking te laten treden is het noodzakelijk dat zowel de verzendende als de ontvangende mailserver STARTTLS ondersteunen.

Wanneer STARTTLS door één van de mailservers niet wordt ondersteund of een versleutelde verbinding niet tot stand kan worden gebracht, kunnen de mailservers teruggevallen op een niet-versleutelde verbinding. Dit wordt *opportunistische encryptie* genoemd. Hoewel dit de afleveringszekerheid van e-mails vergroot, is het een nadeel voor de beveiliging van e-mailverkeer.

Een actieve aanvaller kan STARTTLS blokkeren, een zogeheten STRIPTLS-aanval. Het tot stand brengen van een beveiligde TLS-verbinding gaat via een niet-versleutelde verbinding. Door in het voorstadium de totstandbrenging van de versleutelde verbinding te blokkeren wordt automatisch overgegaan op een niet-versleutelde verbinding. Door deze manipulatie van het berichtenverkeer is het mogelijk om de verbinding af te luisteren en e-mails te lezen. Het is voor actieve aanvallers ook mogelijk om de versleutelingssterkte te verlagen, een downgrade-aanval.

DANE

Bij het maken van een veilige verbinding is een online controle op de authenticiteit van de verzendende partij en de eindbestemming wenselijk. Dit kan door middel van (gepubliceerde) certificaten die door certificaatautoriteiten (CA's) binnen het PKI-stelsel zijn uitgegeven.

DANE maakt het voor de eigenaar van een domein mogelijk om via een met DNSSEC beveiligd DNS-record extra informatie bovenop de offline certificaten aan te reiken. Hierdoor kan real-time een controle worden gedaan op de authenticiteit van de server. Het DANE-record kan gezien worden als een digitale vingerafdruk. Hierdoor kan het naast of in plaats van de certificaten van CA's worden gebruikt. Tijdens de procedure zal dan ook gekeken worden naar de relatie tussen DANE en een PKI.

Toepassing van STARTTLS in combinatie met DANE

Wanneer zowel de verzendende als de ontvangende partij DANE toepassen wordt een verbinding pas tot stand gebracht wanneer het DNS-record van

de verzendende partij gecontroleerd is door de ontvangende partij. Gebruikers van DANE EN STARTTLS worden geadviseerd om de verbinding te verbreken als er geen beveiligde verbinding via STARTTLS opgezet kan worden. Hiermee worden STRIPTLS-aanvallen afgeweerd.

Wie beheert de standaarden?
STARTTLS en DANE worden beheerd door de Internet Engineering Task Force (IETF). IETF is een internationale standaardisatieorganisatie voor internetstandaarden. IETF beheert onder andere ook TLS, DKIM, SPF en DNSSEC.

Waarom is de standaard aangemeld voor pas toe of leg uit?
In 2013 is voor DANE en TLS 1.2 de toetsingsprocedure doorlopen. Omdat DANE nog zeer beperkt werd toegepast en de marktondersteuning voor de toepassing van DANE onvoldoende was heeft de expertgroep geadviseerd om de standaard niet op te nemen op de lijst voor pas toe of leg uit. Onderdeel van het advies was om na een bepaalde periode en op aangeven van de indiener de adoptie van de standaard opnieuw te beoordelen.

In het gesprek met de indiener is naar voren gekomen dat DANE in toenemende mate wordt toegepast met STARTTLS om een beveiligde verbinding tussen mailservers op te kunnen zetten. Daarom wordt op aangeven van de indiener een uitgebreide procedure gevolgd voor STARTTLS, en zal voor DANE aanvullend onderzoek worden gedaan naar de adoptie van de standaard.

Geadviseerd wordt om tijdens de expertsessie te bepalen voor welke lijst(en) de standaarden worden geadviseerd. Mocht bijvoorbeeld blijken dat de adoptie van DANE nog niet voldoende is om de standaard verplicht te stellen, dan kan de standaard ook geadviseerd worden voor de aanbevolen lijst.

(zie ook: *7. Functionele use case*)

3. Criteria voor inbehandelname

Om een standaard in behandeling te nemen moet de standaard vallen binnen de scope van de lijst. Hiervoor gelden drie criteria:

1. Is de standaard toepasbaar voor elektronische gegevensuitwisseling tussen (semi-)overheidsorganisaties en bedrijven, tussen (semi-)overheidsorganisaties en burgers of tussen (semi-)overheidsorganisaties onderling?
Ja. De standaarden hebben betrekking op het tot stand brengen van een beveiligde verbinding bij mailservers, waardoor veilige elektronische gegevensuitwisseling zoals e-mail plaats kan vinden vanuit (semi-

)overheidsorganisaties richting burgers, bedrijven en andere (semi-)overheidsorganisaties.

2. Is het beoogde functioneel toepassingsgebied en het organisatorisch werkingsgebied van de standaard, voldoende breed om substantieel bij te dragen aan de interoperabiliteit van de (semi-)overheid?
Ja. De standaarden zijn algemeen toepasbaar, ook binnen het werkgebied van de (semi-)overheid.

3. Is het zinvol de standaard op te nemen, gezien het feit dat deze niet al wettelijk verplicht is voor het beoogde functioneel toepassingsgebied en organisatorisch werkingsgebied?
Ja. De standaarden zijn niet wettelijk verplicht en opname op de lijst kan helpen om de adoptie van de standaarden verder te bevorderen.

Conclusie
De standaarden voldoen aan de criteria voor inbehandelname.

4. Toetsing kansrijkheid procedure

Het Forum Standaardisatie wil voorkomen dat er standaarden in procedure worden genomen, waarvan bij voorbaat al bekend is dat deze in de expertronde of consultatieronde zullen stranden op één van de inhoudelijke criteria. Daarom heeft de procedurebegeleider de beantwoording van de criteriavragen nagelopen, waar mogelijk zelf aangevuld en vervolgens besproken met de indiener.

1. Open standaardisatieproces
De ontwikkeling en het beheer van de standaard moeten op een open, onafhankelijke, toegankelijke, inzichtelijke, zorgvuldige en duurzame wijze zijn ingericht.

STARTTLS en DANE worden beiden beheerd door de Internet Engineering Task Force (IETF). IETF is een internationale standaardisatieorganisatie voor internetstandaarden. IETF heeft open beheerprocessen. Naast STARTTLS en DANE beheert IETF onder andere ook TLS, DKIM, SPF, IPv6 en DNSSEC. Het specificatiedocument en documentatie over het ontwikkel- en beheerproces zijn kosteloos en voor een ieder te downloaden van de website van IETF (www.ietf.org).

Het gebruik van de standaarden is gratis. Verschillende werkgroepen werken aan de (door)ontwikkeling van standaarden. Samenwerking binnen deze werkgroepen gebeurt veelal via e-mail. Gebruikers en andere belanghebbenden kunnen zich via de website van IETF kosteloos aanmelden voor de werkgroepen. Er hebben voor zover bekend geen

Nederlandse (overheids)organisaties meegewerkt aan de (door)ontwikkeling van de standaarden.

2. Toegevoegde waarde
De interoperabiliteitswinst en andere voordelen van adoptie van de standaard moeten overheidsbreed en maatschappelijk opwegen tegen de kosten, de risico's en nadelen. Voor elk van de te onderscheiden stakeholders (overheid, bedrijven en burgers) afzonderlijk zouden de baten voor de informatievoorziening en de bedrijfsvoering op moeten wegen tegen de kosten. Verder moeten de risico's aan overheidsbrede adoptie van de standaard (beveiliging, privacy) acceptabel zijn.

De toepassing van DANE en STARTTLS maakt het mogelijk om een beveiligde verbinding voor e-mailverkeer tot stand te brengen. Hierdoor is het voor aanvallers niet mogelijk om berichtenverkeer 'af te luisteren' of te manipuleren. Hierdoor kan de ontvangende partij er vanuit gaan dat de e-mail via een beveiligde verbinding is verstuurd vanaf de mailserver van de authentieke en geverifieerde verzendende partij.

Daarnaast biedt het gebruik van DANE de eigenaar van een domein de mogelijkheid om een extra verificatiemiddel, naast de certificaten van CA's, in te zetten.

Tijdens de expertbijeenkomst dient aandacht besteed te worden aan de implementatiekosten en beheerlast van DANE en STARTTLS.

Er worden geen risico's gezien voor overheidsbrede adoptie van de standaard, zoals beveiligings- en privacyrisico's.

3. Draagvlak
De standaarden worden momenteel in Nederland gebruikt door onder andere Netlabs, NLnet en het Forum Standaardisatie. Daarnaast wordt de aanmelding ondersteund door het NCSC en Surfnet.

Met betrekking tot gebruik ondersteunen een toenemend aantal (web)mailproviders STARTTLS, waaronder Google (Gmail), Microsoft (Outlook en Live), XS4ALL en mailbox.org. In de meeste gevallen is het enkel 'onder water' zichtbaar wanneer het opzetten van een TLS-verbinding door middel van STARTTLS mislukt en wordt terug gevallen op een niet-beveiligde verbinding. Google is op dit moment bezig om een terugval op een niet-beveiligde verbinding inzichtelijk te maken in de interface van Gmail.

Er zijn tools beschikbaar voor het aanmaken van DANE-records, waaronder hash-slinger (Redhat) en Idns-dane (NLnet Labs). Het gebruik van DANE is nog minder inzichtelijk en zal nader moeten worden bekeken.

4. Opname bevordert adoptie
De opname op de lijst moet een geschikt middel zijn om de adoptie van de standaard te bevorderen.
Beide standaarden zijn aangemeld voor opname op de lijst met open standaarden. Uit het aanvullend onderzoek voor DANE moet gekeken worden naar de huidige adoptie van de standaard bij Nederlandse (semi-)overheidsinstellingen. Wanneer blijkt dat het gebruik van de standaard niet de omvang heeft die nodig is om de impact en kwaliteit van de standaard te meten (en dus het gebruik van de standaard te verplichten), kan er bijvoorbeeld ook voor gekozen worden om DANE als aanbevolen standaard op te nemen.

Conclusie
Er is op voorhand een mogelijk struikelblok te verwachten. De adoptiegraad van DANE is ten tijde van dit schrijven niet helder. Mocht blijken dat de adoptie van DANE nog niet voldoende is om de standaard in combinatie met STARTTLS verplicht te stellen, dan kan de standaard ook geadviseerd worden voor de aanbevolen lijst of alleen STARTTLS op te nemen met een verwijzing naar DANE. Dit is wenselijk gezien de toegevoegde waarde van DANE bij het gebruik van STARTTLS. Overigens geldt dit natuurlijk ook andersom.

5. Samenhang

Forum Standaardisatie wil weten of de aangemelde standaard samenhangt met standaarden die reeds op de lijst zijn opgenomen, of standaarden die voor toetsing in aanmerking komen. Uit de intake moet duidelijk worden of dit gevolgen heeft voor de toetsing en eventuele opname van de aangemelde standaard.

1. *Bestaat er samenhang tussen de aangemelde standaard en de verplichte ('pas-toe-of-leg-uit') standaarden die reeds op de lijst zijn opgenomen en wat betekent dit voor de toetsing en eventuele opname van de standaard?*
   STARTTLS maakt naast DANE, gebruik van TLS. TLS is een protocol dat tot doel heeft om beveiligde verbindingen op de transportlaag over het internet te verzorgen door middel van cryptografie. DANE maakt direct gebruik van DNSSEC, een standaard voor het registreren en in de Domain Name Server (DNS) publiceren van internet-domeinnamen (zogenaamde 'signing').

   Daarnaast kennen de standaarden samenhang met DKIM, SPF en DMARC. Deze set van e-mailstandaarden hebben als doel misbruik van de domeinnaam middels e-mail te verminderen en/of te voorkomen. DKIM koppelt een e-mail aan een domeinnaam met behulp van een digitale handtekening. SPF controleert of een e-mailserver gerechtigd is om namens het opgegeven e-maildomein

e-mail te verzenden. DMARC is een standaard die het voor organisaties mogelijk maakt om beleid op te stellen over de manier waarop ontvangende e-mailproviders, die DMARC ondersteunen, om zouden moeten gaan met e-mail waar door middel van SPF en/of DKIM niet kan worden vastgesteld dat deze afkomstig is van het eigen domein.

STARTTLS en DANE zorgen er voor dat de verbindingen waarover deze versleutelde en beveiligde e-mails worden verstuurd ook beveiligd zijn.

Verder kennen STARTTLS en DANE samenhang met IPv6 (en diens voorganger IPv4).

STARTTLS en DANE conflicteren niet met deze standaarden. Tijdens de procedure is het belangrijk om deze samenhang inzichtelijk te maken. Bijvoorbeeld aan de hand van een infographic.

2. *Bestaat er samenhang tussen de aangemelde standaard en de aanbevolen standaarden die reeds op de lijst zijn opgenomen en wat betekent dit voor de toetsing en eventuele opname van de standaard?*
   STARTTLS en DANE kennen samenhang met het DNS-protocol, een standaard die URL's vertaalt naar IP-adressen zodat hosts op het netwerk elkaar kunnen vinden.

3. *Bestaat er samenhang tussen de aangemelde standaard en standaarden die in aanmerking komen voor opname op de lijst en wat betekent dit voor de toetsing van de standaard(en)? (Denk bijvoorbeeld ook aan een gezamenlijke toetsing met (een deel van) deze aanvullende standaarden)*
   Zoals aangegeven is initieel alleen DANE aangemeld voor opname op de lijst met verplichte standaarden. Omdat DANE in toenemende mate wordt toegepast met STARTTLS wordt geadviseerd dat een uitgebreide toetsing wordt gedaan voor STARTTLS, en voor DANE aanvullend onderzoek naar de adoptiegraad van de standaard.

6. Sponsorschap

De aanmelding van standaarden voor de lijst van het Forum en het Nationaal Beraad dient ondersteund of gesponsord te worden door

overheids- en/of (semi)publieke organisaties die de standaard reeds in gebruik hebben (of voornemens zijn dit te doen) en die de beoogde opname op de lijsten ondersteunen. Dit draagt bij aan het draagvlak voor de standaard, geeft zicht op de functionele usecase voor de overheid en helpt bovendien om tijdens de toetsing de juiste experts te benaderen.

1. *Welke overheden en/of (semi) publieke organisaties ondersteunen de aanmelding van de standaard?*
   Het NCSC en SURFnet ondersteunen de aanmelding van DANE en STARTTLS.

2. *Hebben deze organisaties de standaard geïmplementeerd? (zie ook punt 7 voor een uitwerking)*
   Het is ten tijde van de intake niet duidelijk of één van bovengenoemde partijen de standaard ook hebben geïmplementeerd. In Nederland maken Netlabs, NLnet en Forum Standaardisatie gebruik van beide standaarden. In Duitsland, Noorwegen en Amerika worden beide standaarden op grotere schaal toegepast. In Duitsland is DANE opgenomen in de technische richtlijn voor 'secure e-mail transport' van het Bundesamt für Sicherheit in der Informationtechnik (BSI). Dit federale bureau is vergelijkbaar met het Forum Standaardisatie.

7. Functionele use case

Voor de standaard dient een duidelijke use case beschikbaar te zijn op basis waarvan overheden en/of instellingen uit de (semi) publieke sector kunnen bepalen of de aangemelde standaard voor hen relevant is en wie eventueel moet deelnemen aan de experttoetsing van de standaard.

De toepassing van STARTTLS en DANE is met name relevant voor (semi-)overheidsorganisaties die veel per e-mail communiceren met burgers, bedrijven en andere (semi-)overheidsinstellingen. Hierbij kan gedacht worden aan gemeenten, uitvoeringsorganisaties (zoals Belastingdienst, DUO, UWV, SVB en DNB), provincies en ministeries. Zonder het gebruik van STARTTLS en DANE wordt (beveiligde) e-mail via een niet-versleutelde en onbeveiligde verbinding verzonden. Voor derden is het dan alsnog mogelijk om dit berichtenverkeer 'af te luisteren' of zelfs te manipuleren. Gevoelige gegevens zoals creditcardnummers of inloggegevens voor DigiD en eHerkenning kunnen hierdoor in het bezit van derden komen.

Door het gebruik van de standaarden wordt de verbinding tussen de verzendende en ontvangende mailserver beveiligd, waardoor het voor derden niet meer mogelijk is om tijdens het transport van een e-mail in te breken. Ook kan de ontvangende partij er vanuit gaan dat de e-mail via een beveiligde verbinding is verstuurd vanaf de mailserver van de

authentieke en geverifieerde verzendende partij. Daarmee wordt het systeem van sleutels en certificaten voor berichtenverkeer veel robuuster.